

# **NAVAL POSTGRADUATE SCHOOL**

## **Monterey, California**



## **THESIS**

**AN INTRODUCTION TO  
CERTIFICATION AND ACCREDITATION  
FOR NEW ACCREDITORS**

by

Natalie Stauffer

June 2003

Thesis Advisors:

Karen Burke  
Craig Rasmussen

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> June 2003	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> An Introduction to Certification and Accreditation for New Accreditors			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Stauffer, Natalie				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b>  The certification process can be defined as a comprehensive evaluation of all security features, both technical and non-technical, of an information system. This process ensures that the system design and implementation meets a distinct set of prescribed security requirements. The accreditation of a system ensures that networks, applications, and operating systems that make up the system are running at an acceptable level of risk. The Designated Approving Authority (DAA) is responsible for deciding what systems to approve for accreditation, and assumes the responsibility for running the accredited system at an accepted level of risk. This analysis of the certification and accreditation process stresses the vital aspects of the process that are of special concern to the DAA. The mission drives the process, and influences the ultimate accreditation decision. The DAA must understand the fundamental aspects of the certification effort, and be able to weigh factors such as the funding, time, and other resources available for the effort, as well as understand the scope of the system as a whole. This thesis covers the vital aspects of certification and accreditation, and provides the new DAA with a guide to the process.				
<b>14. SUBJECT TERMS</b> certification and accreditation, DAA, DITSCAP			<b>15. NUMBER OF PAGES</b> 68	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**AN INTRODUCTION TO  
CERTIFICATION AND ACCREDITATION FOR NEW ACCREDITORS**

Natalie Stauffer  
Civilian, Naval Postgraduate School  
B.S., California State University, Monterey Bay, 2000

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN COMPUTER SCIENCE**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2003**

Author: Natalie Stauffer

Approved by: Karen Burke  
Co-Advisor

Craig Rasmussen  
Co-Advisor

Peter Denning  
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

The certification process can be defined as a comprehensive evaluation of all security features, both technical and non-technical, of an information system. This process ensures that the system design and implementation meets a distinct set of prescribed security requirements. The accreditation of a system ensures that networks, applications, and operating systems that make up the system are running at an acceptable level of risk. The Designated Approving Authority (DAA) is responsible for deciding what systems to approve for accreditation, and assumes the responsibility for running the accredited system at an accepted level of risk. This analysis of the certification and accreditation process stresses the vital aspects of the process that are of special concern to the DAA. The mission drives the process, and influences the ultimate accreditation decision. The DAA must understand the fundamental aspects of the certification effort, and be able to weigh factors such as the funding, time, and other resources available for the effort, as well as understand the scope of the system as a whole. This thesis covers the vital aspects of certification and accreditation, and provides the new DAA with a guide to the process.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

<b>I. INTRODUCTION .....</b>	<b>1</b>
<b>A. RESEARCH QUESTIONS .....</b>	<b>2</b>
<b>B. SCOPE OF RESEARCH .....</b>	<b>2</b>
<b>C. METHODOLOGY .....</b>	<b>3</b>
<b>II. BACKGROUND .....</b>	<b>7</b>
<b>A. THE CERTIFICATION AND ACCREDITATION PROCESS .....</b>	<b>7</b>
1. Roles and Responsibilities .....	10
<b>B. SECURITY CONTROLS AND REQUIREMENTS .....</b>	<b>11</b>
1. DoD Instruction 8500.2, Information Assurance (IA) Implementation .....	11
<i>a. Auditing</i> .....	14
<i>b. Access Control</i> .....	15
<i>c. End User Training</i> .....	15
<i>d. Configuration Management</i> .....	16
2. DCID 6/3 .....	16
<b>III. DETAILED ANALYSIS OF CERTIFICATION AND ACCREDITATION ACTIVITIES .....</b>	<b>19</b>
1. Definition: Phase 1 Tasks .....	20
2. Validation: Phase 2 Tasks .....	22
3. Verification: Phase 3 Tasks .....	24
4. Post Accreditation: Phase 4 Tasks .....	26
<b>IV. CRITICAL COMPONENTS OF THE CERTIFICATION AND ACCREDITATION PROCESS .....</b>	<b>29</b>
<b>PHASE 1 .....</b>	<b>30</b>
<b>V. CONCLUSIONS .....</b>	<b>41</b>
<b>LIST OF ACRONYMS .....</b>	<b>45</b>
<b>REFERENCES .....</b>	<b>47</b>
<b>INITIAL DISTRIBUTION LIST .....</b>	<b>49</b>

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	Phase 1 Key DAA Activities .....	30
Figure 2.	Phase 2 Key DAA Activities .....	32
Figure 3.	Phase 3 Key DAA Activities .....	35
Figure 4.	Phase 4 Key DAA Activities .....	39

THIS PAGE INTENTIONALLY LEFT BLANK

**LIST OF TABLES**

Table 1.           Table 1. Applicable IA Controls by Mission Assurance Category and Confidentiality  
                          Level [From 3]. .....13

Table 2.           Certification Levels and Weights [From 1].....31

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

I would like to thank Craig Rasmussen and Karen Burke for their continual guidance, direction and inspiration. I wish to express gratitude to Cynthia Irvine and George Dinolt for their suggestions, encouragement, and sound advice throughout my experience here at the Naval Postgraduate School.

I would like to thank the National Science Foundation and the Federal Cyber Corps program for providing me with the opportunity to further my education in the computer science field. I would also like to thank personnel at DISA, SPAWAR, NSA, and BAE Systems for taking time to meet with me regarding their experiences with the certification and accreditation process.

Finally, I am grateful to my parents, Cheryle, Randy, and Anne, for their endless patience and support. Thank you, Jill, for inspiring me to achieve more than I ever thought possible. I would like to express my appreciation to Rex, Jeff, Kate, Greta and Iphigenia for their emotional support, understanding, and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

## **I. INTRODUCTION**

The certification process can be defined as a comprehensive evaluation of all security features, both technical and non-technical, of an information system. This process ensures that the system design and implementation meets a distinct set of prescribed security requirements. The accreditation of a system ensures that networks, applications, and operating systems that make up the system are running at an acceptable level of risk based on the results of the certification process. The Designated Approval Authority (DAA) is the executive with the formal responsibility of authorizing the operation of a system. The DAA is responsible for deciding what systems to approve for accreditation, and assumes the responsibility for running the accredited system or network at an accepted level of risk.

Although the DAA is an executive with the authority to evaluate the system and approve it for accreditation, he or she usually has little knowledge of computer security functions. Ensuring that all facets of the certification process have been explored, and that the access, integrity, availability, functionality, and performance of the system are acceptable, is a difficult task.

The background of the DAA is usually that of upper management. Thus, the DAA relies on others for technical advice as it pertains to the computers and systems for which they are responsible. Relying on technical advisors and the people whom the DAA hires to consult on various system design principles and procedures can lead to communication problems and misunderstandings. For example, if the technical advisor to the DAA cannot communicate the concepts entailed in the certification process or relate the notion of residual risk to the DAA in a clear and concise non-technical manner, the DAA will not be adequately informed or prepared to make the appropriate accreditation decision.

For reasons such as this it is important to educate the DAA on how to understand the evaluation of a particular certification and accreditation process to ensure it meets all prescribed requirements. This can be accomplished by providing proper guidance and education to the DAA, as well as by facilitating communication between the DAA and

the technical staff. Because each certification and accreditation process has unique characteristics, this thesis should in no way be considered a checklist or alternative to the rigorous certification and accreditation process already in use. Instead, it will solidify and document the key concepts of the certification and accreditation process to clarify the key factors and aid the DAA in making an informed decision.

## **A. RESEARCH QUESTIONS**

The following questions were used to guide the research and development of this thesis:

1. How does one decide which factors of the certification and accreditation process are key and which are secondary?
2. What is the justification for labeling those pieces left out of as not vital?
3. What are the main roles of the DAA in the certification and accreditation process?

## **B. SCOPE OF RESEARCH**

This thesis will cover the vital aspects of the certification and accreditation process and will provide the new DAA with a tool with which to facilitate the decision about a particular certification. Because the DAA has the formal responsibility of authorizing the operation of a system, this information will ensure that the DAA is fully abreast of all components of the certification and accreditation process before the decision to accredit the system is made. The main goal of this thesis is to provide guidance, to the potential DAA, to foster a better understanding of the process of evaluating a particular system for accreditation.

## C. METHODOLOGY

The information that was collected for this thesis was obtained using the following methods:

- Government Documents:
  - DoD 5200.40 – DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
  - DoD 8510.1-M – DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Manual
  - DoD Directive 8500.1 – Information Assurance (IA)
  - DoD Directive 8500.2 – Information Assurance (IA) Implementation
  - NSTISSI No. 1000 – National Information Assurance Certification and Accreditation Process (NIACAP)
  - OMB Circular A-130, Appendix III
  - NIST Special Pub 800-37 – Guidelines for the Security Certification and Accreditation of Federal Information Technology System
  - NCSC-TG-031 - Certification and Accreditation Process Handbook for Certifiers
  - NCSC-TG-029 v1 - Introduction to Certification and Accreditation
- Articles, White Papers and Technical Reports
- Interviews with individuals who have participated regularly in the C & A process

This research was complemented with input from many other sources to help describe the process. The analysis of documents such as the System Security Authorization Agreement (SSAA), which are key in the certification and accreditation process, was used as a tool with which to comprehend the process on a higher level. This, coupled with the interviews and the literature, aimed to describe the main role and knowledge base of the DAA.

Many papers, articles and documents were reviewed to understand the process in detail. The DITSCAP Manual, 8510.1-M [1], describes the Department of Defense certification and accreditation process. This Manual develops a standard certification and accreditation process for the DoD and supports the DITSCAP 5200.40 document by providing a detailed approach to the activities surrounding the C&A process. The DITSCAP Manual is described in detail in later chapters.

Department of Defense Directive 8500.1 establishes policy and assigns responsibilities to DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare [2]. This directive applies to all DoD systems and establishes policy to ensure that the systems maintain an appropriate level of confidentiality, integrity, and availability. Department of Defense Instruction 8500.2 describes in detail the implementation procedures necessary to achieve the procedures directed in 8500.1. A detailed description of 8500.2 is provided in subsequent chapters [3].

The Office of Management and Budget (OMB) Circular A-130 [4], entitled "Management of Federal Information Resources," establishes policy that Federal agencies must follow when acquiring, using, and distributing government information. This Circular establishes policy for the management of Federal information resources. The appendices contain procedural and analytic guidelines for implementing specific aspects of these policies. Appendix III of OMB A-130 establishes a minimum set of controls to be included in Federal automated information security programs, and assigns Federal agency responsibilities for the security of automated information.

The National Information Assurance Certification and Accreditation Process (NIACAP) is defined by the National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 1000 [5], to establish a standard national process, activities, tasks and management structure to certify and accredit systems that will maintain the information assurance and security posture of a system or site. The NIACAP is used when accrediting non-DoD federal government systems, and is very closely related to the DITSCAP.

The goal of this research was to understand exactly what the DAA should know and understand about the certification and accreditation process in order to adequately approve a system for accreditation. Not only do the technical aspects of a system play a large part in the decision to accredit, but also other things, such as mission, physical security, system boundaries, and the user's level of experience and/or clearances, are all facets of the larger picture that must be understood. The DAA must understand the fundamental aspects of the certification effort, and be able to weigh factors such as the money, time, and resources available for the effort, as well as understand the scope of the system as a whole. The DAA should understand at a high level the requirements of the system, and how these requirements are traced into the system to show compliance. The DAA must be able to trust the Certifier to make sound technical decisions as they relate to the system to be accredited. This trust relationship is a very important factor in the process, because the DAA will be relying upon the Certifier to understand the requirements, perform the tests and evaluations, and report the finding, as well as prepare the accreditation recommendation.

Particular attention was given to the element of subjectivity in the accreditation process. Understanding the subjective aspects of the process is a necessary step in ensuring that the ultimate accreditation decision is the right one. To accomplish this, interviews and meetings with a variety of specialists in the field were performed to further determine specifically which parts of the process may or may not be seen as subjective. This is one reason why the DAA must trust the Certifier to make good decisions. Perhaps a system is compliant with all stated requirements, implements all security policies, but lacks sufficient documentation. It is the responsibility of the Certifier and DAA to decide if this system can be accredited. One Certifier interviewed stated that he would not accredit a system with poor documentation, while another person stated that he had accredited a system with poor documentation with the understanding that the documentation would be updated satisfactorily within a certain time limit. This illustrates the diversity of opinion of the Certifier and DAAs within the accreditation process. The interviews with specialists in the field were further used to analyze how the process is conducted in the "real world". These views will be studied and compared to

understand how much the DAA knows of the subject, and what parts should be explained in more detail.

Further analysis of the certification and accreditation literature, as well as the literature defining the duties and responsibilities of the DAA, will aid in the decision as to which vital pieces of the process should be looked at more closely.

## **II. BACKGROUND**

### **A. THE CERTIFICATION AND ACCREDITATION PROCESS**

The DITSCAP establishes a standardized approach to the certification and accreditation process for the Department of Defense. This document specifies tasks and activities to be performed when evaluating a system for accreditation.

The certification and accreditation process is broken up into four phases, as defined by the DITSCAP. These phases consist of Definition, Verification, Validation, and Post Accreditation. Phase one of the process is Definition. During this phase the system mission is defined, the system boundary, resources, and requirements are determined, and the level of certification is negotiated. The initial draft SSAA is developed, agreed upon, and signed.

This phase contains three key activities: preparation, registration, and negotiation. The preparation activity involves collecting all documents and information pertaining to the system to be accredited. The registration activity begins the risk-management process by identifying the security requirements, system boundary, and level of effort required to complete the certification and accreditation process. The negotiation activity ensures that the SSAA correctly defines the level of effort for the system, as well as that all people involved in the process are familiar with their roles and responsibilities. The SSAA documents the mission and system information, operational and security functionality, operational environment, security policies, system security requirements, known security problems or deficiencies, and other security-relevant information.

The certification level is determined by analyzing the system mission, functions, security requirements, infrastructure, and users. This information will aid in the determination of the degree of confidentiality, integrity, availability and accountability required for the system. The certification Level is determined by the level of confidentiality, integrity, and availability needed in the system. This determination provides the proper degree of assurance that the system will function as specified in the system and security requirements. The DAA should understand the degree of assurance necessary for the system as well as the necessary safeguards required to implement it.

For non-intelligence systems, confidentiality provides protection of information from unauthorized access. Examples of services that help to ensure confidentiality are access control, encryption, object reuse, physical security, TEMPEST techniques, and administrative procedures. These techniques help to prevent unauthorized user access, interception, and emissions. Integrity is preserved by preventing unauthorized users from modifying or deleting information. Access control, digital signatures, configuration control, and physical security are all mechanisms that provide integrity services. Availability is concerned with the system services being accessible and operational on demand by authorized users. The main concern with availability is avoiding denial of service attacks by unauthorized individuals. Access control, backups, modularity, operations security, and redundancy are all forms of protection against denial of service.

The DITSCAP defines four levels of certification. Each level provides a successively rigorous amount of verification techniques to ensure the system behaves as is stated in the requirements definition. Level one requires the completion of the minimum security checklist, which is located in Appendix two of the DoD 8510.1-M. This checklist ensures that the architecture, design, network rules, integrity, life-cycle management, vulnerability assessments, system management, security test and evaluations, and penetration testing of the system have been fully analyzed and reviewed. Levels two, three and four require the completion of the minimal security checklist, as well as independent, in-depth or extensive analysis of the system. These certification levels are selected by analyzing certain characteristics of the system to be certified. These system characteristics are assigned weights that are totaled to give the appropriate certification level.

During this phase of the process, the DAA should regularly review the system to ensure it conforms to the objectives stated in the SSAA. The DAA is also responsible for defining the accreditation requirements, obtaining a threat assessment for the system, assigning a Certifier to conduct the vulnerability and risk assessments, supporting the DITSCAP tailoring and level of effort determination, and approving the SSAA. The Certifier as well as the certification Team will support the DAA in any way they can with his/her responsibilities.

Phase two of the process is Verification. This phase begins with refining or updating the SSAA to reflect any new changes in the system requirements. This phase includes the analysis of the system architecture, software design, network connection rule compliance, products to be integrated into the system, life-cycle management, security requirements validation procedures, and vulnerability assessments.

This analysis of the certification process and security requirements is done to ensure that they are sufficient and correct, as well as to verify that they are relevant to the process and conform to those requirements specified in the SSAA. The certification analysis will also confirm that the system design is implementing the requirements as stated in the SSAA, as well as ensure that the security critical components of the system are working correctly. The last steps in this phase include the development of a Task Analysis Summary Report as well as the evaluation and determination of system certification readiness. The Task Analysis Summary Report summarizes the findings from each of the assessments done during the Certification Analysis and provides recommendations.

During the Verification Phase, the DAA should regularly review the system to ensure it is in accordance with the SSAA. The DAA will also be responsible for overseeing the system evaluation as well as examining the SSAA to make sure that it correctly describes the system, threat, environment, security requirements, vulnerabilities to the system, and all other conditions in which the system will be operating.

The third phase in the process is Validation. This phase validates that the findings in the Definition and Verification phases have led to the creation of a system that performs as stated in the requirements definition, and functions within an acceptable level of residual risk. By this time, the system to be accredited has already been integrated, and is awaiting the official accreditation decision. Again, the SAA will be reviewed, the integrated system will be evaluated, and the final accreditation decision will be made. The System Test and Evaluation (ST&E) are performed during the evaluation to ensure that the security controls for the system are correctly implemented and working efficiently. Risk Assessment and Certification Evaluation Reports are developed and the certification statement is made. The certification statement is the report to the DAA on

the results of the certification testing. This report will include the recommendation to accredit the system or not, or to grant an interim approval to operate (IATO).

The fourth and final phase in the process is the Post Accreditation Phase. At this point the system has already been accredited and must maintain the acceptable level of residual risk that was previously agreed upon. The system is monitored regularly to ensure that there are no significant changes to the configuration or environment that might affect the confidentiality, integrity or availability of the information it contains. This monitoring is performed throughout the lifecycle of the system. Review of any system changes is imperative to ensure that they do not affect the threat level of the system. Changes made must be controlled in such a way as to reflect the stated configuration management requirements. The accreditation of the system is tightly dependent upon the configuration of the system and the way in which it interacts with the hardware and software. Any changes made must be reviewed to ensure they do not invalidate the accreditation decision.

## **1. Roles and Responsibilities**

The main roles in the certification and accreditation process are those of the DAA, Certifier, and user representative. Other roles can be added to support the overall decision process and mission, and are often necessary to ensure that the process is performed as expected, and that the system implements the stated requirements. Often the Program Manager and ISSO will be a part of the process. Each of these roles plays a major part in each phase of the process, and is responsible for determining the scope of the effort as it relates to the mission, resources, architecture and environment. They must all work together to ensure that the project stays on schedule, design meets implementation, and any threats to the system are adequately managed. During phase one of the process it is very important that all roles in the certification effort discuss the security requirements, scope, and level of effort. This discussion should lead to a final agreement by all parties involved.

The DAA is the person with the authority to accredit the system. He or she is usually in upper management and is responsible for evaluating the mission and resources

for the system to be accredited. The DAA approves the system for operating at an acceptable level of residual risk. The amount of residual risk deemed acceptable is dependent upon many factors, most importantly the criticality of the mission. Depending upon mission importance, the residual risk accepted may be significant. It is important to understand that this decision is ultimately a management decision and involves many factors which the Certifier may or may not know of.

The Certifier is responsible for providing the technical expertise of the certification process and explaining all necessary technical information to the DAA. The Certifier may work with a team to conduct the certification process, and must ensure that the security requirements are properly documented in the SSAA. The determination as to the adequate level of residual risk is made by the Certifier, as well as the recommendation as to whether or not the system should be accredited.

The User Representative is concerned with the systems confidentiality, integrity, availability, access, and functionality as it relates to the ultimate mission of the system. The user representative represents the user community and assists in the certification and accreditation process by helping to define the system operations and functional requirements of the system.

The Program Manager manages each aspect of the system from the original concept, to the development, implementation, and system maintenance. The program manager is responsible for the system throughout its entire lifecycle, and is responsible for ensuring the security requirements are implemented correctly.

The Information System Security Officer (ISSO) is responsible for monitoring and maintaining the security of the system as defined by the SSAA, as well as ensuring that the system follows all security requirements as stated in the documentation.

## **B. SECURITY CONTROLS AND REQUIREMENTS**

### **1. DoD Instruction 8500.2, Information Assurance (IA) Implementation**

The Department of Defense Instruction 8500.2 implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of

the DoD information systems and networks as prescribed in the DoD Directive 8500.1. This directive establishes the following responsibilities for the DAAs [3]:

- Ensure that IA is incorporated as an element of DoD information system lifecycle management processes.
- For DoD information systems under his or her purview, ensure that all IA-related positions are assigned in writing, include a statement of IA responsibilities, and ensure that appointees to positions receive appropriate IA training.
- Ensure that all IA Managers meet all access requirements and are U.S. citizens.
- Ensure that IA-related events or configuration changes that might impact accreditation are reported to affected parties.

The responsibilities above, as well as those of the IA Manager, IA Officer, and Authorized users are key aspects of the process and should be understood and followed by the DAA.

This instruction implements an Information Assurance program designed to assess security needs and capabilities, develop security design and configuration that adheres to a common architecture, implement required controls or safeguards, perform system tests and verification, and ensure proper use of configuration management.

Risk management is vital in balancing the importance of the information and supporting technology to DoD missions against the documented threats and vulnerabilities, the trustworthiness of users and interconnected systems, and the effectiveness of IA solutions [3]. This directive explains the many different facets of DoD IA controls and components, such as audit, access control, and configuration management.

Information assurance levels for DoD information systems are assigned explicit IA controls for each system. These levels are defined according to mission assurance category (MAC) and confidentiality level. MACs aim to quantify the IA services of integrity and availability, and scale them according to mission need, with an emphasis on

the “warfighter” needs [3]. MAC I systems require high integrity and high availability, MAC II systems require high integrity and medium availability, and MAC III systems require basic integrity and availability. The confidentiality levels are determined by the classification level of the system (classified, sensitive, public). The mission assurance categories and confidentiality levels are independent of one another; for example, a MAC II system may process classified information while a MAC III system may process public information. There are nine different combinations of mission assurance categories and confidentiality levels. These define nine baseline IA levels. The set of IA Controls applicable to any given DoD information system is a combination of the IA Controls for its mission assurance category and the IA Controls for its confidentiality level. All IA controls for the nine baseline MAC and Confidentiality levels are described in detail in attachments A1 through A6 of the 8500.2 Directive. The following table describes the set of applicable IA Controls for the nine baseline levels.

<b>Mission Assurance Category and Confidentiality Level</b>	<b>Applicable IA Controls</b>
MAC I, Classified	Attachments A1 and A4
MAC I, Sensitive	Attachments A1 and A5
MAC I, Public	Attachments A1 and A5
MAC II, Classified	Attachments A2 and A4
MAC II, Sensitive	Attachments A2 and A5
MAC II, Public	Attachments A2 and A6
MAC III, Classified	Attachments A3 and A4
MAC III, Sensitive	Attachments A3 and A5
MAC III, Public	Attachments A3 and A6

Table 1. Table 1. Applicable IA Controls by Mission Assurance Category and Confidentiality Level [From 3].

This instruction mandates that each DoD information system be reviewed against the stated mission assurance category definitions to determine the appropriate MAC level. The confidentiality level will be assigned based on the classification or sensitivity

of the information processed. These categories and levels determine the appropriate IA controls, and constitute the baseline requirements for IA certification and accreditation or reaccreditation.

The following controls are vital in the operation of any system and are recommended to increase the security and proper functionality of DoD information systems. Depending upon the mission assurance category and confidentiality level assigned to the system, these controls may be supplemented with other controls and components. Higher levels will require more stringent application of controls.

#### *a. Auditing*

The auditing of a system is the process of recording, examining, and reviewing any or all security relevant activities on the system. The information obtained from performing audits is used to detect and deter the misuse of a computer system.

The auditing of the system should include enough information to determine who did what action, the date and time of the action, system location, resources involved, and actions involved. The audit contents should be protected against unauthorized access, deletion, or modification, and should be reviewed at least weekly and kept in backup for any necessary future review. The system should audit successful and unsuccessful logons and logoffs, access to security-relevant objects and directories, such as opens, closes, modifications and deletions, and any other event that might indicate an attempt to violate the security policy of the system [6]. The system should have an appropriate Identification and Authentication (I&A) process to authenticate the user to the system. This will ensure that each user can be associated with an auditable action. I&A will also that ensure only privileged users have access to the system.

Regular review and testing of the audit procedures and policies by the ISSO should be done to ensure that the system is performing as expected. The ISSO can use automated tools to validate that users passwords are sufficient and in compliance with the documented policies, and use intrusion detection devices and other monitoring tools to detect any attacks to the system.

Audit requirements will vary depending upon the classification and certification level of the system. A higher level will require more stringent auditing requirements, testing and documentation. The implementation of the audit requirements will vary depending upon the system in question, as well as the characteristics of the hardware, software, and firmware involved.

### ***b. Access Control***

The use of access control policies will determine who is authorized to access what resources and how. This policy also states who is not authorized to access certain resources. Access control uses password and encryption techniques to ensure that only authorized users have access to the data and programs on the machine. Access control can also segregate programs and data so that the user in question only sees those programs and data that she or he has access to.

### ***c. End User Training***

The end users of the system should be trained well so that they understand the system in question. It is important to provide regular training to all users of the system. This training should be complemented with manuals and other documentation that can be used if they have any future problems or questions. It is also important to educate and train users on security awareness. Employees who are trained and informed of proper security practices and procedures will be better equipped and therefore more trusted to act in such a way as to ensure a more secure environment for the organization. They should understand the importance and details of password creation, security policies and procedures and their individual responsibilities.

DoD Directive 8500.2 states that all DoD employees and IT users shall maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities [3]. They should be capable of appropriately responding to and reporting suspicious activities and conditions, and they should know how to protect the information and IT they access. To achieve this understanding, all DoD employees and IT users

should receive both initial and periodic refresher IA training. Required versus actual IA awareness training shall be a management review item.

#### ***d. Configuration Management***

Configuration management is a vital aspect in the certification and accreditation process. A good team of employees that work together using proper configuration controls will produce a product and/or system that will be more reliable, and thus more secure than the team that does not use configuration management. This will help to ensure that the system does not change throughout the lifecycle. The DAA should appreciate the value and stability that this adds to the life of system.

Configuration management establishes and maintains the integrity of a system throughout its lifecycle. The system requirements are documented, as well as the standards, practices and procedures for the intended configuration management. Version control, revision management, and change process maximize efficiency, and enhance productivity. Configuration management consists of the following four tasks: identification, control, status accounting, and auditing [7]. For every change that is made to an system, the design and requirements of the changed version of the system should be updated and identified. The control task of configuration management is done to ensure that every change made to the documentation, hardware, software or firmware of the system is reviewed and approved by an authorized authority. Status accounting ensures that the configuration of the system or product is evaluated and recorded throughout the life of the system. The configuration audit verifies that the changes made to they system are functionally correct and consistent with the security policy.

## **2. DCID 6/3**

The DoD intelligence community follows the guidelines set forth in the DITSCAP, and provides additional requirements to complement it. These additional requirements are defined in the Director of Central Intelligence Directive 6/3 (DCID 6/3), which explains how to protect sensitive compartmented information within information systems [8].

The DCID 6/3 explains the concepts of Level of Concern and Protection Level, and describes their appropriate use as it pertains to the technical security requirements for confidentiality, integrity and availability in intelligence systems. The Level of Concern ratings are specific for confidentiality, integrity and availability; each is rated at levels Basic, Medium, or High. These Level of Concern ratings are independent of one another.

The DCID 6/3 manual defines the confidentiality of a system and rates the Level Of Concern based on the sensitivity of the information that the Information System stores, maintains, transmits, and processes. The confidentiality level is always rated High in intelligence systems, since all information processed is intelligence information.

The Integrity rating, as defined in the DCID 6/3 [8], is based on the degree of resistance to unauthorized modification of the information maintained, processed, and transmitted by the Information System that is necessary for accomplishing the mission of its users. This rating is highest when a system has the greatest need of resistance from unauthorized modification.

Similarly, the Availability rating is based on the degree of ready availability required of the information maintained, processed and transmitted by the Information System in order to accomplish the mission of its users. This area is rated high when there is a great need for information availability.

Protection Levels in intelligence systems are mainly concerned with the confidentiality of a system. Since the level of concern of any intelligence system must have a high confidentiality rating, the DAA must ascertain the Protection Levels for a system based on the required clearances, formal access approvals and the need-to-know of all users who receive information from the IS without manual intervention and reliable human review [8].

There are five Protection Levels to be considered when accrediting a system. The DCID 6/3 defines the five levels as follows:

- Level 1: All users have the required clearances, formal access approvals, and the need-to-know for all information on the system.

- Level 2: All users have all required clearances and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system.
- Level 3: All users have all required clearances, but at least one user lacks formal access approval for some of the information on the system.
- Level 4: At least one user lacks sufficient clearance for access to some of the information on the IS, but all users have at least a Secret clearance.
- Level 5: At least one user lacks any clearance for access to some of the information on the system.

Each progressively higher level *increases* the risk of loss of classified information, so it is important for the DAA to understand the Protection Levels and their inherent meaning when deciding whether to accredit a system.

In the intelligence community, the DAA often delegates his or her authority to the DAA Representative. The DAA Representative is a technical expert who must ensure the correct operations of system functions and security safeguards, as well as the implementation of the security policy, throughout the lifecycle of the system. The DAA Representative is also responsible for ensuring that all security tests and evaluations are performed, evaluating the perceived threats and vulnerabilities of a system, and maintaining the certification and accreditation documentation, as well as assessing any changes in the system. The DAA Representative is the principal advisor to the DAA, and assumes the responsibility of advising the DAA on all technical information regarding the certification and accreditation process.

### **III. DETAILED ANALYSIS OF CERTIFICATION AND ACCREDITATION ACTIVITIES**

One key goal of this research is to describe exactly what pieces of the process the DAA needs to know to make an informed accreditation decision. This understanding, coupled with that of the DAA's existing knowledge base, will help to further expand the preparedness of the DAA. The DAA should understand the basic concepts of the C&A process, as well as the definition of the minimum requirements that must be met at each certification level.

The mission is key in all certification and accreditation events. Without mission need, there would be no system to accredit. The mission can affect the accreditation decision greatly, so it must be understood that the final choice to accredit the system is a management decision. The C&A process will drive the requirements definition, risk assessment and system evaluation, while the mission will be weighed against residual risk in making the final decision.

The planning and budgeting for certification of a system plays a large role in the process. It is important for the DAA to weigh factors such as cost, time, and resources in order to understand the scope of the problem. Working within budget limitations and determining the appropriate amount of security needed for a system are both vital aspects of the process. The boundaries of the system to be certified, as well as any other external interfaces that may be related to the system but are not within the certification effort, must be fully analyzed.

Each phase of the certification and accreditation process collects vital information that will ultimately lead to the determination of the accreditation decision. Each step in the process is performed to make certain that the requirements match the implementation and that the SSAA correctly reflects the system.

The importance of a tightly coupled relationship between the DAA and the Certifier during the first three phases of the process cannot be understated. The DAA will be relying upon the Certifier for all technical related information of the system, which means that both parties will have a close working relationship. The following

detailed analysis of the tasks associated with the DAA and Certifier shows how closely related their responsibilities are during the certification and accreditation process. Because the Certifier tasks are performed in support of the DAA, the Certifier tasks are listed first in the following discussion of the process. This will succinctly describe the close connection of responsibilities between the Certifier and the DAA, as well as note the close relation of tasks.

## **1. Definition: Phase 1 Tasks**

### **Certifier tasks done in support of the DAA:**

- Support the DAA as technical expert in the certification process.
- Begin vulnerability and risk assessment.
- Tailor the DITSCAP, determine the appropriate level of effort, and prepare the DITSCAP plan.
- Provide level of effort and resource requirements.

### **DAA Responsibilities:**

- Define accreditation requirements.
- Obtain a threat assessment for the system.
- Assign a Certifier to conduct vulnerability and risk assessments.
- Support the DITSCAP tailoring and level of effort determination.
- Approve the SSAA.

Because the Certifier advises the DAA on all technical aspects of the system, it is important that there be a high level of trust between the DAA and the Certifier. The DAA should ensure that the Certifier is experienced with the certification and accreditation process, and has a good background in information assurance.

The negotiation activity is performed during phase one of the certification and accreditation process, and is very important because this is when the scope and level of effort are determined. All people involved in the system development, acquisition, and operation must reach an agreement on the system implementation and how this will be reflected in the system security requirements. There are three tasks to be performed

during the Negotiation activity, as defined in the DITSCAP: conduct the Certification Requirements Review (CRR), agree on the security requirements, level of effort, and schedule, and approve the final phase one SSAA [1].

The DAA should first review the draft SSAA to ensure that all information assurance and security requirements are identified and included. The Certifier, based on the decided level of effort, will conduct an assessment of all technical and non-technical aspects of the system. It will be the Certifier's responsibility to determine and document the tradeoffs between balancing the security risks with the security requirements, resources, and schedule. The CRR is a meeting in which all parties involved in the process decide and agree upon the schedule, cost, level of effort and approach that will be taken during the certification and accreditation process to ensure that all security requirements are met. The SSAA will be reviewed completely to make certain that all necessary and appropriate information is identified.

It cannot be stressed enough how important it is to perform a valid and comprehensive requirements definition during phase one. Everything done during this phase will be used to shape the outcomes for all successive phases. The security requirements should be defined concisely, and should include a security policy.

A Security Requirements Traceability Matrix (SRTM) is used as a tool to refine the understanding of the requirements throughout the entire lifecycle of the system. This tool is used as a repository to which the developers elaborate on the implementation and testing of the requirements. The SRTM will verify that all stated requirements are implemented in the system, and will help to find any problems that may arise from poor requirements definition. Traceability will ensure that the system is complete, as well as provide the basis for future test planning. After the tracing of requirements is finished it is important to do additional testing to ensure that there are no errors in the implementation that were not listed in the requirements. This kind of ad hoc testing will find errors or vulnerabilities that may have been missed in the documentation.

The system description describes in detail the boundaries of the system, as well as system functions, constraints, budget limitations, mission, system users, and the development timeline. System criticality/sensitivity is a measure of the importance and

nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations [9]. To assess this information in context, the system requirements for confidentiality, integrity, and availability must be analyzed.

Risk Management is formally defined as a process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected [1]. This analysis not only examines the threats and risks associated with a particular system, but will be the initial step in describing the necessary resources for the certification effort.

The assessment of the vulnerabilities of, and threats to, the system will define the possible impact that the loss of information will have on the mission. This analysis is used to find the necessary measures to secure the system. During the initial risk analysis, the scope, boundary and methodology of the effort will be defined. This part of the process will begin the groundwork for the certification and accreditation effort. The process of assessing risk will continue throughout the certification effort, assessing each vulnerability and resulting safeguard implementation to ensure cost-effectiveness and reliability. Risk analysis should be applied throughout the system lifecycle at key milestones/decision points (e.g., during requirements definition, completion of architecture, system installation) to aid in the decisions concerning the appropriate level of residual risk.

## **2. Validation: Phase 2 Tasks**

### **Certifier tasks done in support of the DAA:**

- Report certification results to the DAA.
- Provide advice to DAA regarding system readiness for phase three, Validation.

### **DAA Responsibilities:**

- Review system for compliance with the SSAA.
- Support the following certification activities.
  - Oversee the evaluation of the system.

- Review SSAA to ensure it accurately describes the system, threat, environment, security requirements, system vulnerabilities, and all conditions under which the system will be operated.

The SSAA is reviewed at each phase to ensure that it complies with all stated requirements. If any changes are made during system development or modification, or if these changes affect the security posture of the system, this information must be updated in the SSAA. The system evaluation will look at both the functional and security requirements, which were determined in phase one, and make certain that they are being used to shape the design and implementation of the system. The Certifier is responsible for conducting an Initial Certification Analysis to determine whether the system is ready to be tested and evaluated during phase three, Validation. This analysis will ensure that the system functions as stated in the SSAA, that it correctly implements the security requirements, and that all components of the system that are critical to security are functioning properly.

The test plans and procedures, as well as the security specification, will be written in anticipation of phase three, and added to the SSAA. Depending upon the level of certification determined during phase one, the activities involved in the analysis of the system architecture, hardware, software, and firmware design will range from minimal activities to a comprehensive analysis.

Security vulnerabilities and residual risk are evaluated during this phase. Evaluated vulnerabilities are ranked against threat, ease of exploitation, and potential rewards of the exploiter. Threats can be broken down into subgroups as follows:

- **Natural or Environmental Threats** (controlled or uncontrolled)
  - Power Outages
  - Natural Disasters (Earthquake, etc)
  - Fire
- **Human Threats**
  - Accidental
    - Untrained or Poorly trained users
  - Intentional

- Authorized
  - Uncleared users accessing secret information
  - Students accessing faculty information
- Unauthorized
  - Hackers, well-funded adversaries, etc.

A *vulnerability* is defined by NSTISSI No. 4009 to be a weakness in an IS, system security procedures, internal controls, or implementation that could be exploited [10]. Each vulnerability demands specialized attention. During the vulnerability assessment, any inconsistencies that were found during the system evaluation are analyzed to determine how easily they may be exploited. A vulnerability alone does not present a threat to the system. Countermeasures such as access control, audits, personnel security, physical security, and network security can aid in the reduction of known threats.

### **3. Verification: Phase 3 Tasks**

#### **Certifier tasks done in support of the DAA:**

- Identify and assess system vulnerabilities.
- Recommend risk mitigation measures.
- Report certification results to the DAA.
- Provide accreditation recommendation.

#### **DAA responsibilities:**

- Continuously review system for compliance with the SSAA.
- Assess vulnerabilities and residual risk.
- Decide if security safeguards and residual risk are acceptable.
- Approve any corrective actions required.
- Sign accreditation document, decide to accredit, issue IATO, or terminate system operations.

As with all other phases, this phase begins with the DAA reviewing the SSAA to ensure that the system complies with the requirements set forth in the documentation. If

any changes to the system have been made, they must be approved by all parties involved in the certification effort. The tasks performed during the Validation phase are dependent upon the certification level, and done to ensure that the system is functionally ready for operation and will operate at an acceptable level of residual risk.

A detailed vulnerability analysis is done during this phase by means of the Security Test and Evaluation (ST&E) procedure which, as defined by the NIACAP, is an examination and analysis of the safeguards required to protect an IS, as they have been applied in an operational environment, to determine the security posture of that system [5]. This test assesses the technical and non-technical aspects of the security design. During the ST&E, the implementation of security features such as audit trails, intrusion detection systems, physical and technical aspects of access control, contingency planning, automated security tools, policies and procedures, virus programs, and security processing modes are tested to ensure they conform to the stated security requirements and design. If any security problems or vulnerabilities are found during the ST&E, every effort is made to fix the system. After the ST&E is performed, a detailed document is created which contains the results of the evaluation, and information as to the amount of residual risk. Residual risk is the amount of risk remaining after security measures have been applied [5]. It is the DAA who must decide what degree of residual risk is acceptable. It is important that the Certifier assembles the Test Plan and Procedures report and that he or she is an experienced Information Assurance professional. This will ensure that the system has been thoroughly tested and that all documented information has been properly analyzed. The residual risk assessment is key in this phase.

The findings documented during this and the previous phases are consolidated into a report for the DAA. The Certifier must be prepared to explain the findings to the DAA, as well give the system accreditation recommendations. If the system complies with the requirements stated in the SSAA, the Certifier will issue a system certification. This certifies that the system in question correctly implements the stated security requirements. If the Certifier finds any deficiencies in the system, but due to mission needs or other reasons, deems the system can operate at an acceptable level of risk, he or she will recommend an Interim Approval to Operate (IATO) as long as the deficiencies found in the system are fixed within a certain time limit. This is captured in the SSAA.

There are instances in which a system does not meet the stated security requirements and the system cannot operate within an appropriate level of risk; this leads the Certifier to recommend that the system not be accredited.

When the Certifier has documented the system information and has given his recommendation to the DAA, the DAA must review the SSAA and make the final accreditation decision.

#### **4. Post Accreditation: Phase 4 Tasks**

##### **ISSO tasks done in support of the DAA:**

- Periodically review the mission statement, operating environment, and security architecture to determine compliance with the approved SSAA.
- Maintain the integrity of the site environment and accredited security posture.
- Ensure that configuration management adheres to the security policy and security requirements.
- Initiate the C&A process when periodic reaccreditation is required or system change dictates.

##### **Certifier tasks done in support of the DAA:**

- The Certifier is not involved with the process during this phase.
- Support DAA, system operators and ISSO.
- PM will report security related changes in system to DAA and user representative.

##### **DAA responsibilities:**

- Continuously review the system for compliance with the SSAA.
- Review proposed security changes.
- Oversee compliance validation.
- Monitor integrity of system.
- Establish reaccreditation requirements and ensure all assigned systems comply with stated requirements.
- Decide to reaccredit, accredit, or IATO, system if SSAA is no longer valid, or terminate system operations.

To ensure that the system sustains the acceptable level of residual risk determined in all earlier phases, the DITSCAP recommends that activities such as SSAA maintenance, system operations, security operations, configuration management, and compliance validation be performed [1]. This phase begins after a system has been accredited. The Certifier no longer is the main point of contact for the system; that responsibility will shift to the Program Manager. The ISSO and on-site operations staff will ensure that the system maintains the acceptable level of residual risk determined in the certification phases.

Review of any system changes is imperative to ensure that they do not affect the threat level of the system. Changes made must be controlled in such a way as to reflect the stated configuration management requirements. The accreditation of the system is tightly dependent upon the configuration of the system and the way in which it interacts with the hardware and software. Any changes made must be reviewed to ensure they do not invalidate the accreditation decision. The ISSO is responsible for attending configuration management review meetings and relating this information to the Program Manager who in turn is responsible for relating this information to the DAA.

Effective risk-management review is imperative in this phase. Regular evaluations of the threats to the system are an important step in ensuring the system remains secure. The DAA must encourage the ISSO to perform regular evaluations of the system to minimize risk and analyze the performance of the system. The assessment of the system security design and architecture, as well as other requirements defined in the SSAA, should be performed and scrutinized against the system environment and known threats to make certain that the system continues to operate within an acceptable level of residual risk. The system must be evaluated and analyzed periodically to ensure it complies with all requirements. If any changes in the system have been made, the security posture of the system will be in question. Factors that may lead to a change in threats are changes in the system mission, architecture, security policy, system risk, operational mode, audit results and sensitivity levels of the system. The risk management review process is performed to mitigate any possible problems due to changes in the system architecture, policy, or design.

Compliance verification is performed to ensure that the system is functionally operating within the specifications set forth in the SSAA. This will make sure that the system is complying with the security requirements by repeating some tasks that were taken in phase two and three of the process. This involves the validation of tasks and decisions that were made earlier in the process, to ensure that they are being implemented correctly in the system. The DITSCAP recommends that, at minimum the following tasks be performed: Site and Physical security Validation, Security Procedures Validation, System Changes and Related Impact Validation, System Architecture and System Interfaces Validation, Management Procedures Validation, and Risk Decisions Validation [1].

If any changes are made to the system that require re-accreditation, the DITSCAP must be followed from phase one.

#### IV. CRITICAL COMPONENTS OF THE CERTIFICATION AND ACCREDITATION PROCESS

The information obtained through the research and interviews showed that there are many factors of the process that are perceived as vital. All interviewees were asked the same set of questions: when the responses were compiled and analyzed, they revealed a set of very similar answers. These questions framed the discussion during each meeting, and opened the door to many more facets of the process, which lent a deeper understanding and analysis. The subjectivity of the process was given particular attention because this factor is rarely noted in any documentation. This is understandable mainly because subjectivity is not an area with which one likes to associate risk analysis. People like to be assured that the system they are running will correctly implement all requirements, and prefer to think of the implementation process as objective.

The nine main characteristics of the DITSCAP are that it is *tailorable, scalable, predictable, understandable, relevant, effective, evolvable, repeatable, and responsive*. These nine characteristics “provide the flexibility needed to support the diverse DoD mission requirements. A process with these characteristics is essential to integrating information security into the developmental and operational processes of the next generation of DoD systems. This process will permit IS to be evaluated based on mission versus risk in a computing environment where the systems are interdependent and, frequently, interactive”. That the process is predictable ensures that “the process is uniformly applicable to any system. It minimizes personal opinion and subjectivity” [1]. This is the only acknowledgement in the DITSCAP Manual that subjectivity may have a place in the certification and accreditation process. Although the process contains both objective and subjective aspects, the DITSCAP aims to minimize the subjectivity by defining a set of activities and tasks to be performed during each phase of the process. These tasks and activities are followed during each successive phase to ensure the implementation meets the design requirements. At the end of each phase the current system design is verified to ensure it meets all stated requirements. The verification that the system is correctly implementing the requirements at each phase adds a layer of

objectivity to the process, which minimizes any subjectivity that may arise during later phases.

The following analysis of the critical aspects of the process will concentrate on both the subjective and objective pieces of the process, explicitly noting when subjectivity may come into play. There are many key factors of importance to the DAA, which will change depending on mission criticality and the type of system to be accredited. Each phase will be covered in detail, and the vital aspects of the process as it pertains to the DAA will be explained in detail.

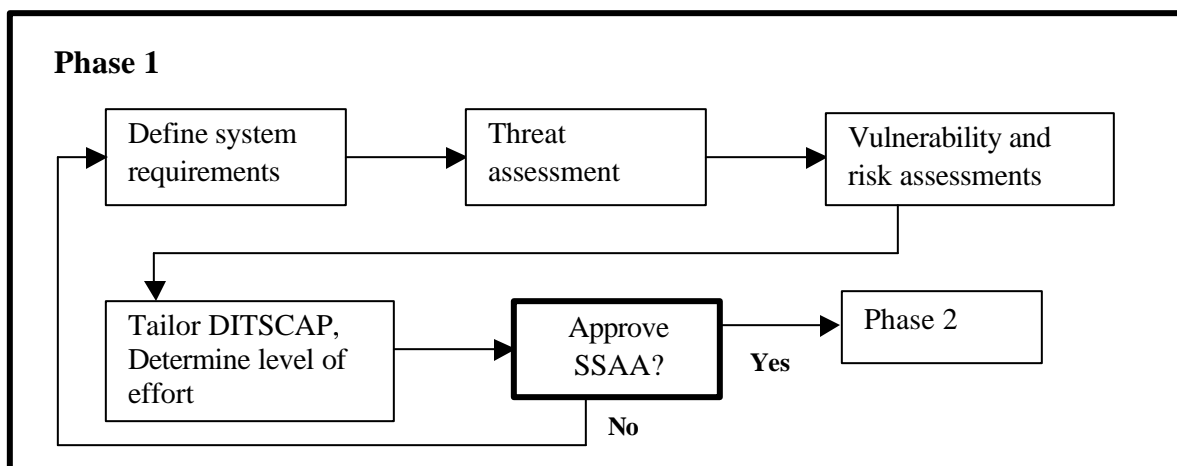


Figure 1. Phase 1 Key DAA Activities

Phase one of the process contains key activities that were explained in detail in previous chapters. System requirements must be defined and understood, a threat assessment for the system must be performed, as well as vulnerability and risk assessments. The tailoring of the DITSCAP and determination of the level of effort for the system certification will be performed, and all activities will lead to the approval of the SSAA.

During the requirements definition phase the DAA should evaluate the cost versus risk tradeoff, as well as make any necessary changes to the security requirements, implementation or procedural controls. The data obtained from the interviews suggested that the DAA does not always have the requisite understanding of the many tradeoffs concerned with resources, time, cost, and risk. The DAA must understand the risks

associated with a system operating in the present environment, and have a firm grasp of how the stated requirements match the certification levels and how the system security controls are validated. The DAA should have a full understanding of the system description and how this maps into the security requirements definition.

OMB Circular No. A-130 defines "adequate security" as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls [4]. Determining the appropriate amount of security will be done by evaluating the results of the risk assessments and system evaluations.

During phase one, a decision as to the certification level will be made and it is important to understand each factor of that decision. In determining the certification level, many factors are considered and given weights, these weights are added together to give the appropriate certification level. In some circumstances, the characteristics of a particular category might dictate a higher classification level than that indicated by the total weights. Among the four certification levels, the weights that identify each level overlap each other. This gives the Certifier some room to add his or her own subjective opinion. This underscores the need for the Certifier to be adequately prepared and experienced in the process to know how to make the appropriate decision. The following table illustrates the overlap of the weights as it pertains to the certification levels:

Certification Level	Weight
Level 1	If the total of the weighing factors are <16.
Level 2	If the total of the weighing factors are 12-32.
Level 3	If the total of the weighing factors are 24-44.
Level 4	If the total of the weighing factors are 38-50.

Table 2. Certification Levels and Weights [From 1]

The determination of the certification level will dictate the amount of analysis done for the system. Choosing the appropriate certification level is crucial in ensuring the proper implementation, security, and requirements for the system. This subjective decision will drive the entire certification and accreditation process. A Level 1 system, as defined in the DITSCAP [1], requires completion of the minimum security checklist. Some professionals interviewed stated that completing the entire checklist for a level 1 system was excessive, while others indicated they may at times do additional analysis. Successive levels require more rigorous testing and analysis of the system, the decision as to the amount of testing done will be made by the Certifier.

After the certification level has been determined, the DITSCAP will be tailored to reflect any specific needs of the system and security requirements. A plan will be created which defines all activities necessary to continue the certification and accreditation process. All of the information compiled thus far will be documented in the draft SSAA. The SSAA must be reviewed by the DAA, as well as the Certifier, to ensure that all controls meet the design of the system. After the SSAA has been reviewed and is approved, the process will proceed to phase two. At this point, all information in the SSAA is finalized and reflects the current state of the system. Once the subjective components at any given phase of the process are bound into the SSAA, they become objective for all successive phases.

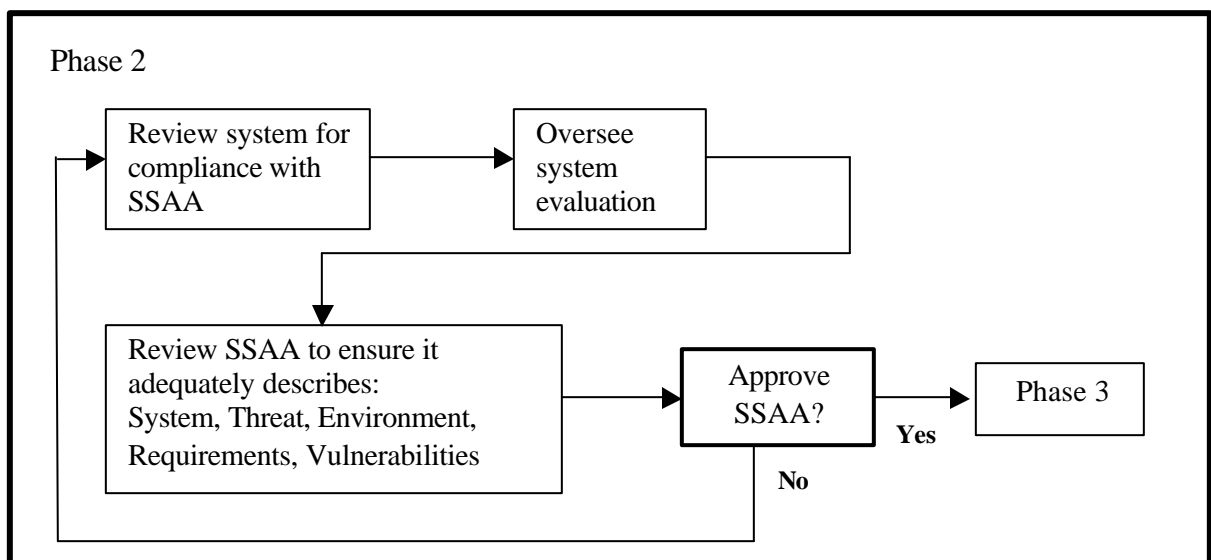


Figure 2. Phase 2 Key DAA Activities

During phase two of the process, the DAA is responsible for first reviewing the system to ensure that it complies correctly with the current SSAA. It is important for the DAA to not only review the SSAA in detail, but to also oversee the evaluation of the system. As stated in earlier chapters, this system evaluation will look at both the functional and security requirements, which were determined in phase one, and make certain that they are being used to shape the design and implementation of the system.

The DITSCAP manual lists certification analysis tasks that must be performed during this phase of the process. These tasks list analyses to be completed, and each task requires different activities that are dependent upon the certification level that was decided during phase one. The higher the level of certification, the more rigorous the analysis of the system will be. For example, the integrity analysis of integrated products evaluates the integration of commercial and governmental off-the-shelf or Non-Developmental Item (NDI) software, hardware and firmware to ensure that their integration into the system design complies with the system security architecture and the integrity of each product is maintained [1]. This integrity analysis will consist of different activities, depending upon the certification level. For a level 1 system, the minimum security checklist must be completed. For successively higher levels, more meticulous tests and analyses will be performed, such as ensuring that the security functionality of each product has been documented. For a level 3 system, in addition to those tasks that must be performed for previous levels, the preservation of product integrity analysis must include configuration control of hardware and firmware components, as well as other very stringent requirements. NCSC-TG-001 states that “Computer systems that process and store sensitive or classified information depend on the hardware and software to protect that information. It follows that the hardware and software themselves must be protected against unauthorized changes that could cause protection mechanisms to malfunction or be bypassed completely. For this reason, changes to trusted computer systems, during their entire lifecycle, must be carefully considered and controlled to ensure that the integrity of the protection mechanism is maintained. Only in this way can confidence be provided that the hardware and software interpretation of the security policy is maintained accurately and without distortion” [6].

It is important for the DAA to understand that the assurance provided by configuration management is beneficial for all systems, not only trusted systems. Configuration Management must be performed adequately and is dependent upon the level of certification. This will ensure that implementation of the system is running as described in the requirements definition, and correctly implementing the security policy.

The DAA must be aware of potential threats and vulnerabilities to the system, as well as understand the different facets of vulnerabilities, such as vulnerabilities caused by hardware, software, data, or humans. The determination of the ease of exploitation must also be understood, as must the residual risk, other related threats, and the probability that the exploitation will occur.

Training of end users is an incredibly important aspect of the process. Users who are properly trained and understand appropriate security related procedures, as well as the consequences of not following the stated policies, are easier to trust to make the right decisions. The insider threat is the most prevalent of all attacks, and should be noted by the DAA. This threat must be countered with tools covered in earlier chapters, such as audit, I&A, and policies.

Comprehensive documentation of the system architecture, requirements, policies, and procedures is necessary in ensuring a positive accreditation decision. Documentation was stressed repeatedly by each person interviewed as one of the most vital aspects of the process. There are many times when poor documentation would lead to a system not getting accredited. Poor documentation could present a problem because this may mean that the team working on the system did not understand the system. Lack of system understanding can lead to poor requirements definition which in turn would lead to the testing and evaluation of a system with poorly defined requirements. If the documentation is lacking purely because the team did not have enough time, perhaps an IATO can be issued with the strict understanding that the documentation will be done within a certain time limit. If there are no training manuals or policies in place, or if the manuals being used are poorly written and uninformative, this would mean that there are many untrained users on the system, which presents another threat, and ultimately would lead to no accreditation of the system. If the system to be accredited is highly trusted, it

will be imperative to have high level, detailed design documents. The DAA must understand the importance of proper documentation for each facet of the system. Detailed documentation and good communication among the team will lead to a better understanding of the requirements and level of effort necessary to complete the process, as well as a relationship where all parties involved can work together to obtain a common goal.

Each task performed in phase two of the process prepares the system for the rigorous validation work to be done during phase three. Again, any changes made to the security posture of the system are documented and updated in the SSAA. The SSAA review is a continual process, which happens throughout each phase and reflects each modification or change to the system.

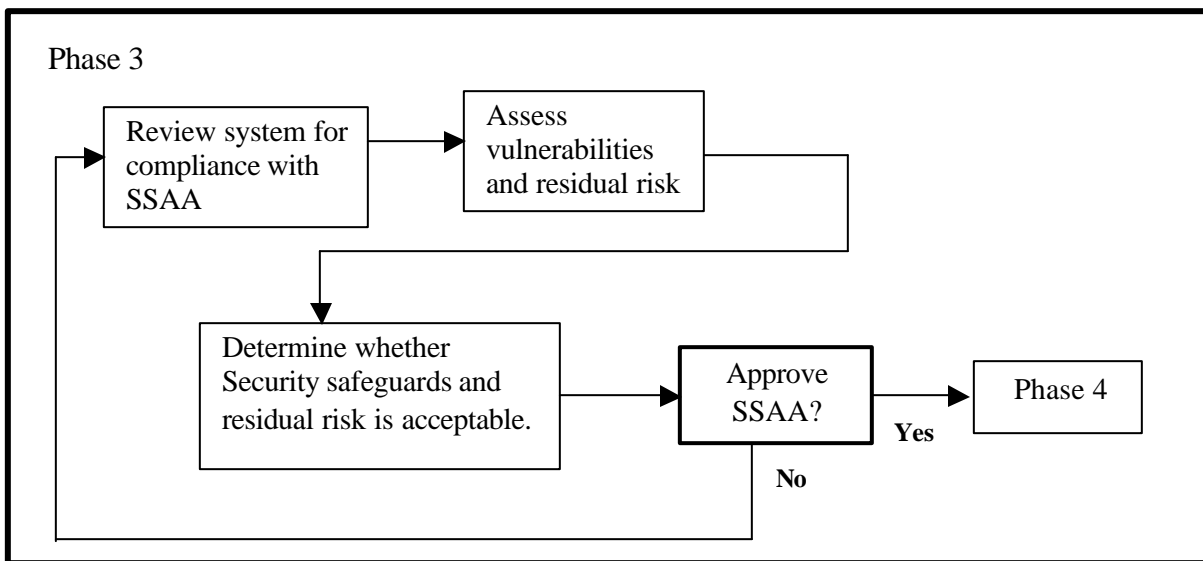


Figure 3. Phase 3 Key DAA Activities

During phase three, the DAA must determine the acceptable level of residual risk for the system. The Naval Risk Assessment Guidebook states “To be effective, risk assessment activities are performed throughout each stage of a system’s life cycle. The output from risk assessments early in a system’s life cycle is used to identify appropriate controls for reducing or eliminating risks. Results of risk assessments performed later in the system’s life cycle are used by the Designated Approving Authority (DAA) to

determine whether a system is adequately protected from risk to allow it to operate conditionally or unconditionally within its specified environment. Risk assessment is therefore a key activity within the DITSCAP” [11].

The risk analysis of a system is a key factor in determining the proper security controls, and helps to add an objective layer to the process. Determining the necessary requirements and evaluating the system in a methodical manner will ensure that the implementation meets the requirements. The risk analysis of a system will review each aspect of the system, and determine all possible risks. When risks are found, countermeasures are developed to reduce or eliminate the risk. These countermeasures will aid in minimizing the risk found during the system analysis. Minimizing risk works to reduce the risk of the system to an acceptable level. Defining the “acceptable level” of risk is again subjective, because each system will have different risk thresholds. The objectivity of this analysis will show how the system security requirements are being met. A risk management matrix can be developed to map the shortfalls of the system, as well as the correctly implemented features. This matrix is used to concisely show the findings of the risk analysis and help aid in the decision as to the appropriate level of residual risk. Examining the findings of the analysis will show what requirements are being met and how, as well as any necessary fixes or changes the system may need. Deciding whether the system adequately meets the requirements will be a decision made by the Certifier and the DAA. This subjective decision will be supplemented with the objective findings of the analysis and evaluation of the system, mission need and criticality, as well as their own experiences with the certification and accreditation process.

It cannot be stressed enough how important the relationship between the DAA and Certifier is. This trust relationship will develop as the process progresses, and the DAA must be assured that the information related to him or her by the Certifier is sufficient and correct. The DAA must examine the summary statement of the risk assessment and understand all risks associated to the confidentiality, integrity, and/or availability of the system. The DAA will not be able to examine the SSAA in full because of its complexity and length. Nevertheless, it is recommended that he or she, at minimum, evaluate the mission need statement, system architecture and overview, and

security policy, as well as the test results from the risk assessment performed in phase two of the process and the residual risk statement.

The DAA should ensure that there are procedures in place for securely operating the system, and that these procedures are adequate. During the Security Test and Evaluation (ST&E) task performed during this phase the security design will be evaluated to ensure the software and hardware features that affect confidentiality, integrity, and availability of the system have been properly implemented as described in the SSAA. The tasks will be performed according to the certification level of the system that was defined during phase one. For a Level 1 system, the Minimum Security Activity Checklist will be performed. For higher levels, more rigorous analysis will be done in addition to completing the checklist. These tasks include higher level evaluations of the security functionality of the system. Level 3 and 4 systems must test the security functions of the system to ensure they verify the integration and operation of all security features. In higher certification levels such as this, it is mandatory to have a Trusted Facilities Manual (TFM) and Security Feature User's Guide (SFUG) available, as well as validated for correctness. The TFM describes the configuration and installation and operation and maintenance of the system, as well as how to effectively use system privileges and protection mechanisms. This manual is written for the system administrator to ensure that he or she has detailed and accurate information pertaining to the system. The SFUG describes the correct system operating procedures according to the system security policy, as well as defines responsibilities to ensure the users of the system are using the system effectively and appropriately. This user guide is written for the general users of the system and should be written in a non-technical manner. It should describe the security mechanisms that the system provides to the user, such as audit and password selection, to ensure that the system is operated as expected [12]. The SFUG and TFM are comprehensive documents that contain procedural information for both the users of the system and the system administrators. The DAA will have to determine the appropriate amount of documented security that defines whether or not there are adequate procedures in place. Monitoring any system changes and ensuring there is adequate configuration management being performed is a necessary step in maintaining a secure system.

The ISSO should be involved in the configuration management process. To verify that the security aspects do not impact the security posture of the system, he or she should be part of the sites process when any changes are to be installed. The Configuration Control Board consists of a body of qualified individuals who are responsible for having meetings pertaining to the configuration management process, as well as giving the final approval for any proposed changes to the system [7]. The ISSO should be an active member of this board, and part of the change process.

The major agreement among all interviewees was that is critically important for the DAA to understand the fundamental attributes of the system to be accredited and the requirements that must be met. Ensuring that the requirements are defined appropriately and validating that the implementation meets the stated requirements are a crucial steps in the accreditation decision. To accomplish them it is recommended that the DAA fully understand the ST&E reports, defined during phase three. Understanding the deficiencies of the system in question, as well as the levels, will aid in giving the DAA an overview of how the system does or does not meet all requirements. The Certifier should ensure that the risk assessment is valid and must translate the findings, as well as the system vulnerabilities and threats, to the DAA.

After the Certifier has documented the complete system information, he or she will give the DAA an accreditation recommendation. By now the requirements have been defined and the system has been tested and evaluated, and it is in the hands of the DAA to make the accreditation decision. The DAA must then review the SSAA and make the final accreditation decision.

The mission criticality of a system now becomes a key factor in the accreditation decision. If the system is critical to the mission, it will have to be accredited. This is one way in which the subjectivity of the process comes into light. All facets of the process will be performed, requirements will be checked to ensure they are implemented properly, tests and evaluations will be done, but ultimately the final decision to accredit may be subjective. Mission justification is defined by the DITSCAP manual as “the description of the operational capabilities required to perform an assigned mission. This includes a description of a system’s capabilities, functions, interfaces, information

processed, operational organizations supported, and the intended operational environment” [1]. The mission, and all information pertaining to it will influence the system environment and security requirements. If the system does not meet all of the requirements stated in the SSAA, but mission criticality is such that the system must become operational, an IATO is issued. The DAA is involved in the details pertaining to the IATO, such as solutions, schedule, security actions, milestones, and duration. The DAA must ensure that the system not only satisfies mission needs, but is operating at an acceptable level of residual risk. The C&A process, although standardized, is flexible enough to allow the system to be evaluated based on mission versus risk tradeoffs. The need for the operational mission, mission risk detailed in any certification findings, and lifecycle costs must be weighed together to determine the appropriate accreditation decision.

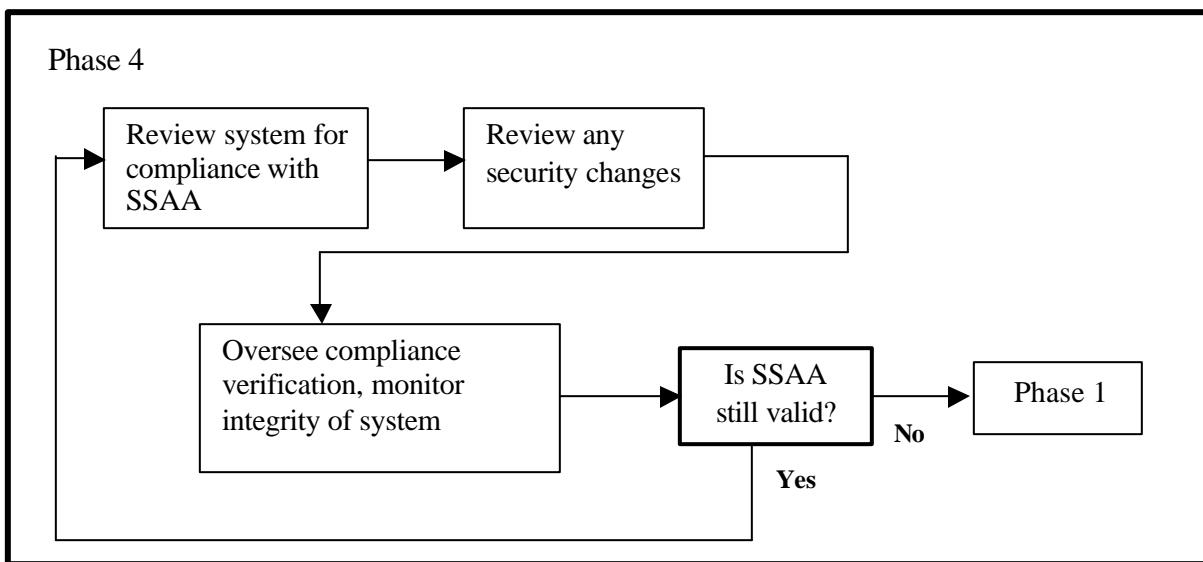


Figure 4. Phase 4 Key DAA Activities

During phase four of the process, the DAA must ensure that the level of security previously defined in the SSAA is maintained. The system is now accredited and operational, and must be maintained and monitored to make certain the implementation continues to meet all stated requirements and that the system operates at the appropriate level of residual risk that was previously defined. The system will be continually observed throughout its life to ensure that its integrity is maintained. The Program Manager is responsible for briefing the DAA with any proposed security changes. The

DAA must ensure that the system performance is regularly evaluated, and if any changes are made to the system that require reaccreditation, the process will return to phase one.

## V. CONCLUSIONS

As the official who assumes responsibility for the residual risk associated with operating the system, the DAA relies heavily on the Certifier to provide an accurate assessment of that risk. The Certifier will perform most of the assessments, analysis, and testing of the system, and will then report the findings to the DAA. Only after being thoroughly briefed of all findings, and developing an understanding of the various details of the system, can the DAA make the accreditation decision. The DAA's role in the certification and accreditation process is continual, beginning with the determination of the level at which the system should be protected, agreement on the system security requirements, and support of the certification activities. This study of the role that the DAA plays in the certification and accreditation process answers one of the main research questions. A second question concerned identification of factors in the C&A process that are of critical importance from the point of view of the DAA. These vital aspects of the process, as it pertains to the DAA, are those pieces that are necessary for a knowledgeable accreditation decision.

The final question concerned items considered nonessential from the point of view of the DAA. The pieces of the process that have been downplayed should in no way be considered to be less than vital to the process as a whole. The rationale for reduced emphasis on these aspects of the process is that the DAA should not be expected to have the time or the resources to know every aspect of the process, but should understand the core aspects of the process and the system in question. The Certifier will relate all technical details of the system to the DAA to ensure that he or she has enough information to make an informed accreditation decision.

The analysis of the certification and accreditation process as it pertains to the DAA stresses the vital aspects of the process that should be looked at more closely. The mission drives the process, and influences the ultimate accreditation decision. Mission criticality is key in defining the level of effort and requirements necessary for the certification and accreditation of the system. The mission justification and mission

criticality will drive the requirements definition as well as the degree of testing and evaluation to which the system will be subjected.

Subjectivity in the process was given particular attention. This was stressed because the presence of subjectivity in the process is largely ignored in the documentation. All parties interviewed agreed that there are some aspects of the process that can be seen as subjective. Ensuring that the necessary and sufficient definition of requirements is done early, and that proper risk analysis and assessment techniques are used, will help to reduce some subjectivity of the process. Although the amount of subjectivity can be decreased, there will always remain decisions that are to some degree subjective. This needs to be understood by both the DAA and Certifier, and underscores the importance of a good working relationship between them. The DITSCAP defines rigorous phases, which ensure that the system design meets the implementation and minimizes the subjectivity of the process even when the mission may dictate otherwise.

Thorough and valid definition of security requirements is a vital aspect of the process. This was agreed upon by all people interviewed, and should be well understood by the DAA. The requirements definition is performed during phase one of the process, and will drive all tasks and activities performed in subsequent phases. Ensuring that the system is correctly implementing the requirements and that the system design meets the system specifications will be determined by those requirements defined during the first phase of the process. Not only will adequate definition of requirements lead to a properly secured system, it will ensure the process is performed correctly.

The objective of the DITSCAP is to establish a standard process, set of activities, general tasks, and a management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense Information Infrastructure (DII). This process supports an infrastructure-centric approach, with a focus on the mission, environment, and architecture [1]. This process is applied to all DoD systems and, when properly conducted, ensures an appropriate level of confidentiality, integrity and availability to make certain that the Defense operations are not disrupted and the DoD missions are accomplished.

The interviews and documentation of the certification and accreditation process led to a deeper understanding of the tasks and activities that surround the process as it pertains to the DAA. These tasks and activities are the cornerstone of the process, and should be understood and performed in detail to ensure the system to be accredited is correctly implementing all stated requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS

C&A	certification and accreditation
DAA	Designated Approval Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
IA	Information Assurance
IATO	Interim Approval To Operate
IS	Information System
ISSO	Information Systems Security Officer
IT	Information Technology
OMB	Office of Management and Budget
RTM	Requirements Traceability Matrix
SFUG	Security Features Users Guide
SRTM	Security Requirements Traceability Matrix
SSAA	System Security Authorization Agreement
ST&E	Security Tests and Evaluation
TFM	Trusted Facilities Manual

THIS PAGE INTENTIONALLY LEFT BLANK

## REFERENCES

- [1] DoD 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), Application Manual," July 2000
- [2] DoD Directive 8500.1 "Information Assurance (IA)," October 2002
- [3] DoD Instruction 8500.2 "Information Assurance (IA) Implementation," February 2003
- [4] Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 1996
- [5] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No.1000, "National Information Assurance Certification and Accreditation Process (NIACAP)," April 2000
- [6] NCSC-TG-001 "A Guide to Understanding Auditing in Trusted Systems," July 1987
- [7] NCSC-TG-008 "A Guide to Understanding Configuration Management in Trusted Systems," March 1988
- [8] Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information Within Information Systems
- [9] National Institute of Standards and Technology (NIST) Special Publication 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," October 2002
- [10] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, "National Information Systems Security (INFOSEC) Glossary," January 1999
- [11] Chief of Naval Operations Information Assurance Publication, Module 5239-16 "Risk Assessment Guidebook," March 2003

- [12] Gordon Army Base “Required Security Documentation,”  
[<http://ia.gordon.army.mil/iaso/lesson7.htm>] June 2003

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dr. Ernest McDuffie  
National Science Foundation  
Arlington, VA
4. RADM Zelebor  
N6/Deputy DON CIO  
Arlington, VA
5. Russell Jones  
N641  
Arlington, VA
6. David Wirth  
N641  
Arlington, VA
7. CAPT Sheila McCoy  
Headquarters U.S. Navy  
Arlington, VA
8. CAPT Robert Zellmann  
CNO Staff N614  
Arlington, VA
9. Dr. Ralph Wachter  
ONR  
Arlington, VA
10. Dr. Frank Deckelman  
ONR  
Arlington, VA
11. Richard Hale  
DISA  
Falls Church, VA

12. George Bieber  
OSD  
Washington, DC
13. Deborah Cooper  
DC Associates, LLC  
Roslyn, VA
14. David Ladd  
Microsoft Corporation  
Redmond, WA
15. Marshall Potter  
Federal Aviation Administration  
Washington, DC
16. Ernest Lucier  
Federal Aviation Administration  
Washington, DC
17. Keith Schwalm  
DHS  
Washington, DC
18. RADM Joseph Burns  
Fort George Meade, MD
19. Howard Andrews  
CFFC  
Norfolk, VA
20. Steve LaFountain  
NSA  
Fort Meade, MD
21. Penny Lehtola  
NSA  
Fort Meade, MD
22. Craig Rasmussen  
NPS  
Monterey, CA
23. Karen Burke  
NPS  
Monterey, CA

24. Natalie Stauffer  
Civilian, Naval Postgraduate School  
Monterey, CA

THIS PAGE INTENTIONALLY LEFT BLANK